

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
NASIMLIWALME@GMAIL.COM;
TALIB@GMAIL.COM;
IRSHAD.CGANIMATOR@GMAIL.COM;
SHAHSAYEDNAQASHHAIDER@GMAIL.
COM; TALIBANSARI067@GMAIL.COM;
AND TANDAR.AFGHAN@GMAIL.COM,
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.

Criminal No. 1:17-sw-178

UNDER SEAL

**APPLICATION FOR ORDER DIRECTING GOOGLE NOT TO NOTIFY
ANY PERSON OF THE EXISTENCE OF A SEARCH WARRANT**

Pursuant to 18 U.S.C. § 2705(b), the United States requests that the Court order Google LLC not to notify any person (including the subscriber or customer of the accounts listed in the search warrant) of the existence of the search warrant issued in this case for another 12 months.

On April 6, 2017, in his affidavit in support of an application for the search warrant in this case, FBI Special Agent Mario A. Fratantonio swore to this Court that disclosure of the search warrant, the affidavit, and/or the application and the attachments thereto would jeopardize the progress of the investigation. In light of that representation, the United States moved this Court, pursuant to 18 U.S.C. § 2705(b), to seal the search warrant materials, and order Google not to disclose the existence of the warrant to the subscribers of the accounts that were searched.

On April 6, 2017, this Court considered the government's submissions, and determined that there was reason to believe that notification of the existence of the search warrant would seriously jeopardize an ongoing investigation, including by giving the targets an opportunity to

flee or continue flight from prosecution, destroy or tamper with evidence or witnesses, change patterns of behavior, or notify confederates. *See* 18 U.S.C. §§ 2705(b)(2), (3), & (5).

Further, this Court found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation, and that no available alternative would suffice to protect the government's legitimate interest in concluding the investigation. Having found that the government's legitimate interest in protecting the investigation outweighed any interest in the disclosure of the material, this Court ordered Google to not disclose the existence of the warrant materials to any person or entity, for a period of two years from the date of the Order (except that Google could disclose the Order to law enforcement officers of the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant).

On December 4, 2019, the United States moved the Court to order the further renewal of the non-disclosure order. On December 6, 2019, this Court ordered Google to not disclose the existence of the warrant for another five months. On April 10, 2020, this Court ordered Google to not disclose the existence of the warrant for another six months. In October 2020, this Court denied the government's motion to extend the non-disclosure order. In its order (attached as Exhibit A to this pleading), the Court stated that the government's application failed to provide any substantive discussion as to the current status of the investigation, whether the investigation has been diligently pursued, or any specific information as to why the disclosure of the warrant to the subscribers of the six email accounts could impede the investigation at this time - - more than three and half years later.

On December 17, Google, LLC notified the FBI that the Google would continue to not disclose to any person or entity the existence of the warrant as long as Google was provided with

a new non-disclosure order by January 16, 2021. Exhibit B. The United States now moves the Court to extend the non-disclosure order for another 12 months.

Pursuant to 18 U.S.C. § 2705(b), we now reiterate our request that the Court extend the ban on notification for an additional 12 months. As seen in Special Agent Fratantonio's affidavit, the warrant at issue relates to the investigation of the kidnapping in 2012 in Afghanistan of American citizen Caitlan Coleman and her husband, Canadian citizen Joshua Boyle. In April 2017, the warrant at issue was used to try to identify the kidnappers.

In October 2017, Coleman and Boyle were rescued by the Pakistani military, but the kidnappers were not captured. Even since their rescue, the FBI has been attempting to identify the kidnappers so that they ultimately can be prosecuted. The reason that the investigation has not been completed in the last eight years is because the individuals who kidnapped Coleman and Boyle, and held them hostage for more than five years, have not yet been captured. An important factor impacting the ability of American authorities to capture them is that they reside in parts of Pakistan and Afghanistan in which the United States cannot readily identify and capture criminal defendants.

Since 2017, the FBI has continued to try to monitor the location of the individuals suspected of involvement in the kidnapping and hostage-holding, in the hopes of being able to find them in a location from which they can be arrested or captured, and then extradited to the United States. So far, the FBI has not found them outside of areas of Afghanistan or Pakistan in which the FBI cannot reach them. The likelihood of them traveling from those areas into places where they can be reached by American authorities likely would be diminished to the extent that they receive notification that such authorities suspect them of involvement in the kidnapping of Coleman and Boyle, and for five years holding them hostage.

In our prior motions, we stated that there was reason to believe that notification of the existence of the warrant would seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Those concerns remain today. The investigation to date indicates that the users of the accounts that are the subject of the warrant were involved in the kidnapping. Any notification suggesting that the FBI is aware of the communications facilities used by the kidnappers or their associates could cause them to significantly change their communications practices and could cause others around them to do their same. Such actions would impair the FBI's ability to identify the kidnappers.

The investigation to date has indicated that the kidnappers are not U.S. persons, but instead citizens of Afghanistan and/or Pakistan. The facts found so far indicate that the only connections of the kidnappers to the United States is their use of internet service providers based in America - - and their kidnapping of an American citizen.

The Supreme Court has held that the Fourth Amendment does not “apply to activities of the United States directed against aliens in foreign territory.” *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267, 271 (1990). Based on the Fourth Amendment’s text, drafting history, and post-ratification history, as well as its own precedents, the Court concluded that the Fourth Amendment was not intended “to restrain the actions of the Federal Government against aliens outside of the United States territory.” *Id.* at 265–67. “If there are to be restrictions on searches and seizures which occur incident to such American action,” the Court explained, “they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.” *Id.* at 275. Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, at least where such persons lack “substantial connections” to

this country, the Fourth Amendment does not require the United States to notify such persons that of the search of their email accounts.

Verdugo-Urquidez involved a physical search that was conducted overseas, while a search of an internet service provider takes place within the United States. The fact that the communications of a non-U.S. person outside the United States may be collected from within the United States is not the kind of “significant voluntary connection with the United States” that brings that person within the Fourth Amendment’s protection under *Verdugo-Urquidez*. 494 U.S. at 271–72. Otherwise, any foreign person abroad seeking to evade U.S. surveillance could claim Fourth Amendment protection simply by communicating through the facilities of service providers located in the United States. That result would be plainly contrary to the Supreme Court’s recognition that the Fourth Amendment protects “the people of the United States” rather than “aliens outside of the United States territory.” *Id.* at 266–67.

Moreover, when the government seizes the emails of a non-U.S. person located abroad, the location of the seizure has no bearing on the person’s privacy interests and should not affect the constitutional analysis. When it comes to the content of communications, “the Fourth Amendment protects people, not places.” *Katz v. United States*, 389 U.S. 347, 351 (1967). Accordingly, there is no “constitutional distinction which depends upon the location” of the seizure. *See United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) (there is no constitutional distinction which depends upon the location of a recording device). Inasmuch as the accountholders and/or users of the account that is the subject of the warrant in this case are non-U.S. persons located abroad, they are not entitled to any notice of the warrant.

Coleman and Boyle were held hostage for over five years, and the investigation into the identity of their kidnappers continues. This investigation is quantitatively different from one

involving a crime that was committed within the United States by United States persons.

Identifying the kidnappers thousands of miles away, and ultimately finding them in a location at which they might be captured, is likely to take far longer than the investigation of a domestic kidnapping takes.

Disclosure of the warrant before the investigation is concluded may hamper the FBI's ability to identify the kidnappers. Accordingly, the United States asks the Court to extend the bar on notification by Google to the subscribers for an additional year in order to protect the integrity of the investigation.

WHEREFORE, the United States requests that the Court grant the attached Order directing Google not to disclose the existence or content of the warrant for an additional 12 months, except that Google may disclose the attached subpoena to its attorney for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss aspects of an ongoing criminal investigation that are not known to all of the targets of the investigation, and premature disclosure may seriously jeopardize that investigation.

Executed on December 20, 2020.

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney



By: _____

Gordon D. Kromberg
Assistant United States Attorney
Phone: 703-299-3721
Email: Gordon.kromberg@usdoj.gov

Attachment A

Attachment B

From: ndonotice@google.com <ndonotice@google.com>
Sent: Thursday, December 17, 2020 11:05 AM
To: Houston, Dana E. (WF) (FBI) <dehouston@fbi.gov>
Subject: [EXTERNAL EMAIL] - [9-0842000029839] Non-Disclosure Order
Expiration Regarding Internal Reference Number 1006374

Hello,

According to our records, the non-disclosure order accompanying your legal process issued April 6, 2017 expired October 10, 2020.

Due to the uncertainty surrounding the Coronavirus (COVID-19) pandemic, Google will extend an additional thirty-day grace period to permit you to get a court ordered extension of this order.

After that grace period, unless we receive a copy of a court ordered extension of this order, we will provide user notification in accordance with our notice policy.

The notification will be sent by email and will include your agency name and a reference number or case number, if applicable. Google may also provide a copy of the legal process if requested to do so.

If you have obtained or intend to obtain an extension, please reply directly to this email and/or include the case identification number located in the subject line. It is important to reference the case identification number in any further communications about this matter so that we can match your correspondence to the correct matter.

To preclude user notification, respond to this email and indicate that you will be seeking an extension of your non-disclosure order.

Regards,
Google Legal Investigations Support

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

APR 6 2017

Alexandria Division

UNDER SEAL

IN THE MATTER OF THE SEARCH OF
ACCOUNTS AT GOOGLE, INC.,
YAHOO, INC., AND FACEBOOK, INC.

)
) Case No. 1:17sw 178
)

Affidavit in Support of Application for a Search Warrant

I, Mario A. Fratantonio, after being duly sworn, depose and state as follows:

1. I was the affiant on the attached affidavit in support of a warrant to search information held by Facebook, Inc., executed on May 26, 2016, relating to the kidnapping of Caitlan Coleman and Joshua Boyle. I hereby incorporate the contents of that affidavit ("the May 26th Affidavit") as though fully set forth herein.

2. This affidavit supports an application for warrants to require the disclosure to the government of the messages and transactional information associated with the following:

a. the email accounts **nasimliwalme@gmail.com; talib@gmail.com; irshad.cgAnimator@gmail.com; shahsayednaqashhaider@gmail.com; talibansari067@gmail.com; and tandar.afghan@gmail.com;** stored at premises owned, maintained, controlled, or operated by email service provider Google, Inc. at 1600 Amphitheatre Parkway, Mountain View, California;

b. the email account **msshagiwal@yahoo.com**, stored at premises owned, maintained, controlled, or operated by email service provider Yahoo! Inc., at 701 First Avenue Sunnyvale, California; and

c. the social media accounts **100014078226915; 100015000011533; 100000618711831; 100000586720074; and 100004905426398**, stored at premises owned, maintained, controlled, or operated by service provider Facebook, Inc., at 1601 Willow Road, Menlo Park, California.

Based on the facts contained herein, there is probable cause to believe that within these messages and transactional information are records, documents, communications, messages, and other

information, more particularly described on Attachment A (and incorporated here), related to communicating threats, in violation of 18 U.S.C. § 875.

3. The information contained in this affidavit is based on my personal knowledge and observations made during the course of this investigation, information conveyed to me by other law enforcement officials, personal review of records, documents, and other physical evidence obtained during this investigation, and information I have gained through my training and experience. Documents referred to herein are from summaries and draft translations; they are not direct quotes. Since this affidavit is submitted for the limited purpose of supporting the search warrant, I have not included every fact known to me concerning this investigation.

I. Probable Cause

4. In addition to the information contained in the May 26th Affidavit, I add the following information. On December 19, 2016, my FBI colleagues found a video posted to Youtube, which portrayed Coleman and Boyle as hostages. According to records provided by Google, Inc., the user who posted the video portraying hostages Coleman and Boyle claimed the email account **nasimliwalme@gmail.com** as the user's contact information. Accordingly, I seek a warrant to search the contents of the email account **nasimliwalme@gmail.com** in order to further identify the user who posted the video of Coleman and Boyle in captivity.

5. After learning that the email account **nasimliwalme@gmail.com** was associated with the user who posted the video that portrayed Coleman and Boyle in captivity, the FBI obtained from Google, Inc. subscriber information for the email account **nasimliwalme@gmail.com**. According to Google, Inc., the email account **nasimliwalme@gmail.com** account was registered by a user who claimed to use (A) the Pakistan-based phone number, 923488434073; (B) the email account **talib@gmail.com**; (C) the email account **irshad.cganimator@gmail.com**; and

(D) Facebook account **100014078226915**. Accordingly, I seek a warrant to search the contents of those accounts in order to further identify the user who posted the video of Coleman and Boyle in captivity.

6. Based on my training and experience, I know hostage takers often use multiple layers of communications security on the internet in order to mask their true identity. For that reason, I obtained subscriber information from service providers for accounts that were linked to the account of the user who posted the video of Coleman and Boyle in captivity.

A. Pakistan-Based Phone Number 923488434073

7. According to the records of Facebook, the Pakistan-based phone number 923488434073 was asserted to be a contact phone number for the user of Facebook account **100015000011533**. Accordingly, I seek a warrant to search the contents of Facebook account **100015000011533** in order to further identify the user who posted the video of Coleman and Boyle in captivity.

8. According to the records of Facebook, Inc., the user of Facebook account **100015000011533** claimed the email address **shahsayednaqashhaider@ gmail.com** as a contact email address. Accordingly, I seek a warrant to search the contents of the email address **shahsayednaqashhaider@ gmail.com** to further identify the user who posted the video of Coleman and Boyle in captivity.

B. The Email Account **Talib@gmail.com**

9. According to the records of Facebook, Inc., the email account **talib@gmail.com** was provided as a contact email address for Facebook accounts **100000618711831** and **100000586720074**. Accordingly, I seek a warrant to search the contents of Facebook accounts

100000618711831 and **100000586720074** to further identify the user who posted the video of Coleman and Boyle in captivity.

10. According to the records of ooVoo (another provider of social media services), the email account **talib@gmail.com** was provided as a contact email address for an account at ooVoo, along with another email address, **talibansari067@gmail.com**. Accordingly, I seek a warrant to search the contents of email account **talibansari067@gmail.com** to further identify the user who posted the video of Coleman and Boyle in captivity.

C. The Email Account **irshad.cganimator@gmail.com**

11. According to the records of Facebook, Inc., the email address **irshad.cganimator@gmail.com** was provided as a contact email address for Facebook account **100004905426398**. Accordingly, I seek a warrant to search the contents of Facebook account **100004905426398** to further identify the user who posted the video of Coleman and Boyle in captivity.

12. According to the records of Facebook, Inc., Facebook account **100004905426398** was registered by a user claiming as contact information the email account **irshad.cganimator@gmail.com** and **tandar.afghan@gmail.com**. Accordingly, I seek a warrant to search the contents of email account **tandar.afghan@gmail.com** to further identify the user who posted the video of Coleman and Boyle in captivity.

D. Facebook account Facebook **100014078226915**

13. According to the records of Facebook, Inc., Facebook account **100014078226915** was registered by a user claiming as contact information the email accounts **msshagiwal@yahoo.com** and **nasimliwalme@gmail.com**. Accordingly, I seek a warrant to

search the contents of email accounts **msshagiwal@yahoo.com** and **nasimliwalme@gmail.com** to further identify the user who posted the video of Coleman and Boyle in captivity.

II. Yahoo! Inc.

14. Based on my training and experience, I know the following about Google, Inc., and Yahoo! Inc.:

- a. Google, Inc. is the internet service provider for email accounts using the suffix "gmail.com." Yahoo! Inc. is the internet service provider for email accounts using the suffix "yahoo.com." Each company requests subscribers to provide basic information, such as name, gender, zip code and other personal/ biographical information, but does not verify the information provided. Google, Inc. is located at 1600 Amphitheatre Parkway, Mountain View, California. Yahoo! Inc. is located at 701 First Avenue, Sunnyvale, California.
- b. Google, Inc. and Yahoo! Inc. each maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include opened and unopened e-mail, account access information, e-mail transaction information, and account application information;
- c. Subscribers of Google, Inc. and/or Yahoo! Inc. may access their accounts on servers maintained and/or owned by their service provider from any computer connected to the Internet located anywhere in the world;
- d. Stored electronic communications, including opened and unopened e-mail for their subscribers may be located on computers of Google, Inc. or Yahoo! Inc. Any e-mail that is sent to a subscriber of either company is stored in the subscriber's "mail box" on the company's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the servers of the internet service provider indefinitely;
- e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to a server of the internet service provider, and then transmitted to its end destination. Users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at their service provider, but

that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

- f. A subscriber of services from Google, Inc., or Yahoo! Inc. can store files, including e-mails and image files, on servers maintained and/or owned by their internet service provider; and
- g. A subscriber of Google, Inc. or Yahoo! Inc. may store e-mails and/or other files on a server of their internet service provider for which there is insufficient storage space in the subscriber's computer and/or which he does not wish to maintain in the computer in his residence. As a result, a search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the server of their internet service provider.

15. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google, Inc., Yahoo, Inc. and Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Paragraphs A and B of Attachment A. Upon receipt of the information described in Paragraphs A and B of Attachment A, government-authorized persons will review that information to locate the items described in Section C of Attachment A.

16. I am trained and experienced in identifying communications relevant to the crimes under investigation, but personnel of Google, Inc., Yahoo, Inc. and Facebook are not. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence, but employees of Google, Inc., Yahoo, Inc. and Facebook are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Google, Inc., Yahoo, Inc. and Facebook for the relevant account and then

to analyze the contents of that account on the premises of those corporations. Further, the impact on the businesses of that corporation would be severe.

17. Accordingly, executing a warrant to search an e-mail account at Google, Inc., Yahoo, Inc. and Facebook requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject e-mail account in this case for evidence of the target crime will require that agents cursorily inspect all e-mails produced by Google, Inc., Yahoo, Inc. and Facebook in order to ascertain which contain evidence of that crime, just as it necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to identify all of the information subject to seizure, because keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

18. In order to facilitate seizure by law enforcement of the records and information sought from Google, Inc., Yahoo, Inc. and Facebook through this affidavit and application with a minimum of interference with the business activities of Google, Inc., Yahoo, Inc. and Facebook to protect the rights of the subject of the investigation, and to effectively pursue this investigation, this application seeks the issuance of a warrant that would permit employees of Google, Inc., Yahoo, Inc. and Facebook to assist agents in the execution of this warrant, in accordance with the procedures described in Attachment A to the warrant, which is hereby incorporated into this affidavit. In accordance with these procedures:

- a) The search warrant for the Google, Inc., accounts will be presented to Google, Inc. personnel, who will be directed to isolate the accounts
nasimliwalme@gmail.com; talib@gmail.com; irshad.cgAnimator@gmail.com

**shahsayednaqashhaider@gmail.com; talibansari067@gmail.com;
tandar.afghan@gmail.com.**

- b) The search warrant for the Yahoo, Inc., accounts will be presented to Yahoo, Inc. personnel, who will be directed to isolate the accounts **msshagiwal@yahoo.com.**
- c) The search warrant for the Facebook, Inc., accounts will be presented to Facebook personnel, who will be directed to isolate the accounts **100014078226915;
100015000011533; 100000618711831; 100000586720074; 100004905426398.**
- d) In order to minimize any disruption of computer service to innocent third parties, employees of Google, Inc. Yahoo, Inc., or Facebook, Inc., and/or law enforcement personnel trained in the operation of computers will create and provide to law enforcement personnel in electronic form an exact duplicate of the identified accounts and all information stored in those accounts.
- e) Law enforcement personnel will thereafter review all information and records received from employees of Google, Inc. Yahoo, Inc., and/or Facebook, Inc. to determine the information to be seized by law enforcement personnel. The information to be seized consists of information that constitutes evidence of relates to communicating threats, in violation of 18 U.S.C. § 875, including records relating to the identities of those who created, used, or communicated with the account(s).

19. I am advised that this Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

Conclusion

20. Based on the foregoing, there is probable cause to believe that within the messages and transactional information associated with the following:

a. the email accounts **nasimliwalme@gmail.com; talib@gmail.com;
irshad.cganimator@gmail.com; shahsayednaqashhaider@gmail.com;
talibansari067@gmail.com; tandar.afghan@gmail.com;** stored at premises owned, maintained, controlled, or operated by email service provider Google, Inc. at 1600 Amphitheatre Parkway, Mountain View, California;

b. the email account **msshagiwal@yahoo.com**, stored at premises owned, maintained, controlled, or operated by email service provider Yahoo! Inc., at 701 First Avenue Sunnyvale, California; and

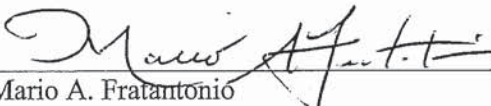
c. the social media accounts **100014078226915**; **100015000011533**; **100000618711831**; **100000586720074**; and **100004905426398**, stored at premises owned, maintained, controlled, or operated by service provider Facebook, Inc., at 1601 Willow Road, Menlo Park, California;

there are records, documents, communications, messages, and other information, more particularly described on Attachment A, related to communicating threats, in violation of 18 U.S.C. § 875.

21. Wherefore, I request the issuance of search warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure allowing agents to seize the information stored on the server of Google, Inc., Yahoo, Inc. and Facebook, as described above, and in accordance with the search procedure described in Attachment A.

22. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal.

FURTHER THIS AFFIANT SAYETH NOT.


Mario A. Fratantonio
Special Agent, Federal Bureau of Investigation

Subscribed to and sworn before me on this 6th day of April 2017.


_____/s/_____
John E. Anderson
United States Magistrate Judge
JOHN E. ANDERSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A (Google, Inc.)

A. The search warrant will be presented to Google, Inc. personnel who will be directed to isolate the accounts for the electronic mail accounts **nasimliwalme@gmail.com; talib@gmail.com; irshad.cganimator@gmail.com; shahsayednaqashhaider@gmail.com; talibansari067@gmail.com; tandar.afghan@gmail.com**. Google, Inc. employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of these accounts, including an exact duplicate of all information stored in the computer accounts and files described therein.

B. Google, Inc. shall provide to the agent who serves the search warrant in electronic form the exact duplicate of the accounts for the electronic mail addresses **nasimliwalme@gmail.com; talib@gmail.com; irshad.cganimator@gmail.com; shahsayednaqashhaider@gmail.com; talibansari067@gmail.com; tandar.afghan@gmail.com** and all information stored in those accounts and files, including:

1. All electronic mail stored and presently contained in, or on behalf of, the electronic mail addresses and/or individual accounts identified above;
2. All existing printouts from original storage of all of the electronic mail described above;
3. All transactional information of all activity of the electronic mail addresses and/or accounts described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;
4. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or accounts described above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and
5. All records indicating the services available to subscribers of the electronic mail addresses and/or accounts described above.

C. Law enforcement personnel will thereafter review all information and records received from the Google, Inc. employees to determine the information to be seized by law enforcement personnel. The information to be seized consists of information that constitutes evidence of relates to communicating threats, in violation of 18 U.S.C. § 875, including records relating to the identities of those who created, used, or communicated with the accounts.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
NASIMLIWALME@GMAIL.COM;
TALIB@GMAIL.COM;
IRSHAD.CGANIMATOR@GMAIL.COM;
SHAHSAYEDNAQASHHAIDER@GMAIL.
COM; TALIBANSARI067@GMAIL.COM;
AND TANDAR.AFGHAN@GMAIL.COM;
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.

Criminal No. 1:17-sw- 178

UNDER SEAL

**ORDER TO SEAL AND FOR
NONDISCLOSURE PURSUANT TO 18 U.S.C. § 2705(b)**

The United States, pursuant to Local Rule 49(B) of the Local Criminal Rules for the U.S. District Court for the Eastern District of Virginia and 18 U.S.C. § 2705(b), having moved to seal the search warrant, application, supporting affidavit, motion to seal, and this Order, and having further moved for a § 2705(b) nondisclosure order covering these materials;


The Court, having considered the government's submissions, including the facts presented by the government to justify sealing; having determined that there is reason to believe that notification of the existence of these materials will seriously jeopardize the ongoing investigation, including by giving the targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence or witnesses, change patterns of behavior, or notify confederates, if any, *see* 18 U.S.C. §§ 2705(b)(2), (3), & (5); having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing; finding none would suffice to protect the government's legitimate interest in

concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED that the United States' motion is GRANTED, and the search warrant, application, supporting affidavit, motion to seal, and this Order be SEALED until further order of the Court.

IT IS FURTHER ORDERED under 18 U.S.C. § 2705(b) that Google, Inc. or its affiliates shall not disclose the existence of these materials to any person or entity, for a period of two years from the date of this Order, except that Google, Inc. may disclose this Order to law enforcement officers of the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant. This non-disclosure order is subject to further renewal upon a proper showing under 18 U.S.C. § 2705(b).

Date: April 6, 2017

_____/s/ 
John F. Anderson
United States Magistrate Judge
JOHN F. ANDERSON
UNITED STATES MAGISTRATE JUDGE

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
NASIMLIWALME@GMAIL.COM;
TALIB@GMAIL.COM;
IRSHAD.CGANIMATOR@GMAIL.COM;
SHAHSAYEDNAQASHHAIDER@GMAIL.
COM; TALIBANSARI067@GMAIL.COM;
AND TANDAR.AFGHAN@GMAIL.COM,
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.

Criminal No. 1:17-sw- 178

UNDER SEAL

**UNITED STATES' MOTION TO SEAL AND
FOR 18 U.S.C. § 2705(b) NONDISCLOSURE ORDER**

The United States of America, pursuant to Local Rule 49(B) of the Local Criminal Rules for the U.S. District Court for the Eastern District of Virginia, now asks for an order to seal the search warrant, application, supporting affidavit, and this motion and proposed order, until the United States makes a motion to unseal these materials. In addition, pursuant to 18 U.S.C. § 2705(b), the United States asks this Court to order Google, Inc. not to disclose the existence of these materials except to the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant until such time as the materials are unsealed.

I. Reasons for Sealing (*See* Local Rule 49(B)(1))

1. At the present time, law enforcement officers of the Federal Bureau of Investigation are conducting an investigation into violations related to communicating threats, in violation of 18 U.S.C. § 875.

2. Premature disclosure of the specific and sensitive details of this ongoing investigation would jeopardize this ongoing criminal investigation, including by giving the

targets an opportunity to flee prosecution, destroy or tamper with evidence and witnesses, change patterns of behavior, and notify confederates, if any. In addition, given the nature of the crimes under investigation and the status of the investigation, the specific details of the evidence included in the affidavit necessarily contain sensitive law enforcement information about an ongoing and proactive investigation. If such information were made public at this time, it would jeopardize the ongoing investigation by alerting the person suspected of engaging in criminal conduct of undercover law enforcement activity and other information known to law enforcement. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. The Governing Law (*See* Local Rule 49(B)(2))

4. It is generally recognized that the public has a common-law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrants and orders issued pursuant to 18 U.S.C. § 2703. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 292 (4th Cir. 2013); *Media Gen. Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005). To substantively overcome the common law presumption of access to search warrant materials, a court must find that there is a “significant countervailing interest” in support of sealing that outweighs the public’s interest in openness. *In re Application*, 707 F.3d at 293, *citing Under Seal v. Under Seal*, 326 F.3d 479, 486 (4th Cir. 2003).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. *Ashcraft v. Conoco, Inc.*, 218 F.3d 288, 302 (4th Cir. 2000).

6. Regarding the notice requirement in the specific context of search warrants, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” *Media Gen. Operations*, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” *Id.* Accordingly, in the context of search warrants, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” *Id.* at 430 (quoting *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. Finally, regarding the requirement of specific findings, the Fourth Circuit’s precedents state that “in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” *Media Gen. Operations*, 417 F.3d at 430 (quoting *Goetz*, 886 F.2d at 65), so long as the ultimate “decision to seal the papers . . . [is] made by the judicial officer,” *Goetz*, 886 F.2d at 65. Moreover, “[i]f appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” *Id.* at 65; see also *In re*

Wash. Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“[I]f the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal.”). The government’s interest in sealing may be supported by a desire to maintain the secrecy of the investigation, preventing the potential subject from being tipped off, or altering behavior to thwart the government’s ongoing investigation. *In re Application*, 707 F.3d at 293.

III. Period of Time the United States Seeks to Have Matter Remain Under Seal (*See* Local Rule 49(B)(3))

8. Pursuant to Local Rule 49(B)(3), the search warrant materials will remain sealed until the need to maintain the confidentiality of these materials and the related investigation expires, after which time the United States will move to unseal the materials.

9. Notwithstanding this motion to seal, the United States requests authorization to provide copies as necessary to execute the application.

IV. Reasons for Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b)

10. Pursuant to 18 U.S.C. § 2705(b), this Court may order Google, Inc. not to notify any other person or entity (including any customer) of the existence of a search warrant issued pursuant to § 2703 for such times as this Court deems appropriate, so long as this Court finds that there is reason to believe such notification would result in, among other factors, “flight from prosecution,” “destruction of or tampering with evidence,” or “otherwise seriously jeopardizing an investigation.” *Id.* at §§ 2705(b)(2), (3), & (5).

11. In this case, there is reason to believe that notification to any person or entity of the existence of the search warrant would result in flight from prosecution and destruction of or tampering with evidence or witnesses. This is because the investigation is ongoing and because the subjects, who are unaware of this aspect of the ongoing

investigation, may, upon becoming aware of this aspect of the investigation, flee or destroy and delete electronic and other evidence of their illegal actions. In addition, a notified subject may also alert other subjects involved in the criminal activity, if any, thus seriously jeopardizing the investigation.

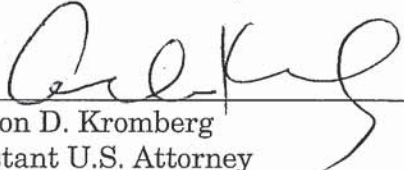
WHEREFORE, the United States respectfully requests that the search warrant, application, supporting affidavit, and this motion and proposed order, be sealed until the United States makes a motion to unseal. The United States further requests that the Court order Google, Inc. not to notify any person or entity, including any of its customers, of the existence of the search warrant and related materials except to law enforcement officers of the Federal Bureau of Investigation as part of its cooperation with law enforcement agents to execute the search warrant, pursuant to 18 U.S.C. § 2705(b), for the period of two years from the date of this Order, subject to renewal upon a proper showing under 18 U.S.C. § 2705(b).

Date: April 5, 2017

Respectfully submitted,

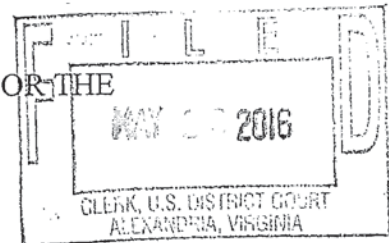
Dana J. Boente
United States Attorney

By:


Gordon D. Kromberg
Assistant U.S. Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNDER SEAL

IN THE MATTER OF THE SEARCH OF
INFORMATION MAINTAINED BY
FACEBOOK, INC.

)
)
)

No. 1:16sw 287

I, Mario A. Fratantonio, after being duly sworn, depose and state as follows

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since August 2008. I am currently assigned to the Washington Field Office. I have training in the preparation, presentation and service of criminal complaints and arrest and search warrants, and have been involved in the investigation of numerous types of offenses against the United States, including crimes of terrorism. Prior to my employment as a Special Agent, I worked within the FBI's Counterterrorism Division as an Intelligence Analyst. In such a capacity, I was responsible for analyzing various terrorist threats and assisting with the development of threat mitigation strategies. My knowledge of the facts and circumstances contained within this affidavit are based upon my personal knowledge and investigation, my training and professional experiences concerning the use of social media in criminal activity, and translations provided by a FBI linguist.

2. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require Facebook, Inc., a social networking company headquartered at 1601 S. California Avenue, in Palo Alto, California, to disclose to the government all content and other information associated with (i) Facebook Account **100011407980766** and the Facebook user name "Hodeman Mujahid" and (ii) Facebook Account **100009118829119** and the Facebook user name "Mahajir Zalmi", collectively referred to herein as the "Subject Facebook Accounts". Based on the facts contained herein, there is probable cause to believe that within the Subject Facebook Accounts are records, documents,

communications, messages, and other information, more particularly described on Attachment A, related to the communication of threats, in violation of 18 U.S.C. § 875.

3. This affidavit is based upon my personal knowledge and investigation, my training and professional experiences concerning the use of social media in criminal activity, and translations provided by a FBI linguist. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

I. Probable Cause

A. The Haqqani Network

4. According to publically available online materials published by the National Counterterrorism Center, the Haqqani Network is a Sunni Islamist militant organization founded by Jalaluddin Haqqani, who emerged as a top Afghan warlord and insurgent commander during the anti-Soviet war. Jalaluddin later allied with the Afghan Taliban as that group's Minister of Tribal and Border Affairs when the Taliban held power in Afghanistan during the mid-to-late 1990s. He was a known associate of Usama Bin Ladin and was recognized as one of Bin Ladin's closest mentors during the al-Qa'ida founder's formative years in the 1980s Afghan war. Sirajuddin Haqqani is Jalaluddin's son, and along with several of his closest relatives, currently leads the day-to-day activities of the group.

5. The Haqqani Network is primarily based in North Waziristan, Pakistan, and conducts cross-border operations into Afghanistan. The group is primarily composed of members of the Zadran tribe. The Haqqanis are considered the most lethal and sophisticated insurgent

group targeting US, Coalition and Afghan forces in Afghanistan, and typically conduct coordinated small-arms assaults coupled with rocket attacks, Improvised Explosive Devices (IEDs), suicide attacks, and attacks using bomb-laden vehicles.

6. The Haqqani Network is responsible for some of the highest-profile attacks of the Afghan war, including the June 2011 assault on the Kabul Intercontinental Hotel, conducted jointly with the Afghan Taliban, and two major suicide bombings—in 2008 and 2009—against the Indian Embassy in Kabul. In September 2011, the Haqqanis participated in a day-long assault against major targets in Kabul, including the U.S. Embassy, International Security Assistance Force (ISAF) headquarters, the Afghan Presidential Palace, and the Afghan National Directorate of Security headquarters.

7. In September 2012, the U.S. Secretary of State designated the Haqqani Network as a Foreign Terrorist Organization because of its involvement in the Afghan insurgency, attacks on U.S. military and civilian personnel and Western interests in Afghanistan, and because of its ties to the Taliban and al-Qa'ida. In July 2015, the media reported the Mullah Akhtar Mansour, the leader of the Afghan Taliban, appointed Sirajuddin Haqqani as one his two deputies and, thus, openly formalized and acknowledged the relationship between the Taliban and the Haqqani Network.

8. Anas Haqqani is the brother of Sirajuddin Haqqani and was a fundraiser for the Haqqani Network. Anas Haqqani was detained by Afghan government authorities in October 2014 and, as of the authoring of this affidavit, remains in Afghan custody.

B. The Kidnapping of Caitlan Coleman

9. In October 2012, Caitlan Coleman, a U.S. citizen from Pennsylvania, apparently was kidnapped with her husband, Canadian citizen Joshua Boyle, by Taliban militants in

Afghanistan. After they were kidnapped, Caitlan and Joshua apparently were placed within the custodial care of the Haqqani Network.

10. In July 2013, someone claiming direct access to members of the Afghan Taliban emailed Caitlan's father a video of his daughter and her husband, Joshua Boyle. In the video, Caitlan stated that she was being held prisoner by the Taliban.

11. According to Caitlan's father, in late January 2014, the International Committee of the Red Cross advised him that, in the course of a recent meeting with members of the Taliban, the Taliban members acknowledged holding Caitlan and Joshua captive; they reported that Caitlan gave birth to a baby while in captivity.

C. Facebook Postings by Mahajir Zalmai and Hodeman Mujahid

12. On April 19, 2016, at least 64 people were killed and hundreds others were wounded when an office of the Afghan Government's National Directorate of Security was attacked in Kabul. Shortly after the attack, the Taliban claimed responsibility for the operation on its Pashto-language and English-language websites.

13. Open sources suggested the Afghan Government blamed the Haqqani Network for planning the attack. On April 20, 2016, Rahmatullah Nabil, a former director of the Afghan Government's National Directorate of Security, was quoted as saying that, to prove its seriousness in the fight against terrorism, the Afghan government should immediately hang Anis Haqqani.

14. On April 21, 2016, the FBI identified a previously unreleased photograph of Caitlan and Joshua in connection with a Facebook post associated with the Facebook user name Mahajir Zalmai and Facebook account **100009118829119**. According to an FBI linguist who translated the Pashto text that accompanied the photograph, Facebook user Mahajir Zalmai

and/or the user of Facebook account **100009118829119** posted a statement implicitly threatening the lives of Caitlan and Joshua if Anas Haqqani was executed (essentially stating that, before deciding to execute Anas Haqqani, the Afghan government should consider the fate of Caitlan and Joshua).

15. That same day, the FBI identified the same previously unreleased photograph of Caitlan and Joshua in connection with a Facebook post associated with the Facebook user name Hodeman Mujahid and Facebook account **100011407980766**. According to an FBI linguist who translated the Pashto text that accompanied the photograph, Facebook user Hodeman Mujahid and/or the user of Facebook account **10001407980766** posted another statement that implicitly threatened the lives of Caitlan and Joshua if Anas Haqqani was executed (essentially stating that “if we find out that you have harmed the Emirates prisoners . . . then pray for your own sake [good] and the sake [good] of these poor guys”).

16. I believe the referenced Facebook postings were in response to Nabil’s call for hanging Anas Haqqani. Therefore, I believe the users of Facebook Account **100011407980766** with the user name Hodeman Mujahid, and Facebook Account **100009118829119** with the user name Mahajir Zalmai conveyed threats to kill Caitlan and Joshua on behalf of the Taliban or Haqqani Network, in violation of 18 U.S.C. § 875.

17. Based upon my knowledge and experience, photographs and/or videos of hostages are typically produced by their captors, in this instance the Taliban and/or Haqqani Network. Therefore, anyone possessing photographs of Caitlan and Joshua, particularly the posted photograph which was not publicly available until April 21, 2016, either had direct or indirect access to the captor network. Therefore, Facebook Account **100011407980766** with the user name Hodeman Mujahid, and Facebook Account **100009118829119** with the user name

Mahajir Zalmi likely have some degree of access to the parts of the Taliban and/or Haqqani Network who are holding Caitlan and Joshua captive.

D. Facebook, Inc.

18. Based on my training and experience, I know that Facebook, Inc. is a company with offices at 1601 S. California Avenue, in Palo Alto, California, and that owns and operates a free access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Each Facebook user account has a unique Facebook user identification number (UID).

19. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

20. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account

includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

21. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

22. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

23. Facebook has a Photos application, where users can upload an unlimited number of albums and photos and videos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he receives a notification of the tag and a link to see the photo or video. For Facebook's

purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

24. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

25. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

26. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

27. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

28. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

29. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

30. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

31. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

32. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

33. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

34. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

35. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

36. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. I know that social networking providers

such as Facebook, Inc. can maintain email messages and other information associated with user accounts for long periods of time, and that it is not uncommon for messages to be accessible through such service providers for months and even years after they were initially sent, received, or posted.

37. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

38. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on Facebook's servers associated with the Subject Facebook Accounts will contain evidence, fruits, and instrumentalities of the Subject Offense, as more fully described in Attachment A. In particular, I believe the Subject Facebook Accounts are likely to contain evidence of the identities and locations of the users of the Subject Facebook Accounts and their co-conspirators, including but not limited to the identification of others who are responsible for the kidnapping and/or captivity of Caitlan and Joshua.

II. Information to be Searched and Things to Be Seized

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require Facebook, Inc. to disclose to the government copies of the records and other information (including the content of communications) associated with the Subject Facebook Accounts that is stored at the premises of Facebook, Inc. The records should include but not be limited to:

- (a) All contact and personal identifying information, including passwords, security questions and answers, and screen names;

- (b) All activity logs and all other documents showing the user's posts and other Facebook activities, and all photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them
- (c) All Photoprints and Neoprints, including profile information and all photos uploaded by that user ID or by any user that have that user tagged in them, News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; all past and present friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (d) All records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests, as well as records of communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken; and all privacy settings and other account settings, and all records showing which Facebook users have been blocked by the account;;
- (e) All "check ins" and other location information, and all IP logs, including all records of the IP addresses that logged into the account;
- (f) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked" and all information about the Facebook pages that the account is or was a "fan" of; and all records of Facebook searches performed by the account, and all information about the user's access and use of Facebook Marketplace;
- (g) All records of the length of service, the types of service utilized by the user, and the means and source of any payments associated with the service, and all cookie data and associate machines and accounts collected by Facebook for user's account to include, but not limited to, browser information if available and other pages and groups where the user (or the associated user) is the creator.

40. I am trained and experienced in identifying communications relevant to the crimes under investigation, but the personnel of Facebook, Inc., are not. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital

evidence, but employees of Facebook, Inc., are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Facebook, Inc. for the relevant account and then to analyze the contents of that account on the premises of that company. Further, the impact on the businesses of Facebook, Inc. would be severe.

41. Accordingly, executing a warrant to search an account at Facebook, Inc. requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject account in this case for evidence of the communication of threats will require that agents cursorily inspect all information produced by Facebook, Inc. in order to ascertain which contain evidence of those crime, just as it necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to identify all of the information subject to seizure, because keywords search text, but many common files on Facebook do not store data as searchable text.

42. In order to facilitate seizure by law enforcement of the records and information sought through this affidavit and application with a minimum of interference with the business activities of Facebook, Inc., to protect the rights of the subject of the investigation, and to effectively pursue this investigation, this application seeks the issuance of a warrant that would permit employees of Facebook, Inc., to assist agents in the execution of this warrant, in accordance with the procedures described in Attachment A to the warrant, which is hereby incorporated into this Affidavit. In accordance with the procedures described in Attachment A to the warrant:

- a. The search warrant for the Facebook, Inc. account will be presented to Facebook, Inc. personnel who will be directed to isolate the information associated with accounts **100011407980766** ("Hodeman Mujahid") and **100009118829119** ("Mahajir Zalmi").
- b. In order to minimize any disruption of computer service to innocent third parties, Facebook employees and/or law enforcement personnel trained in the operation of computers will create and provide to law enforcement personnel in electronic form an exact duplicate of the identified information;
- c. Law enforcement personnel will thereafter review all information and records received from Facebook, Inc. employees to determine the information to be seized by law enforcement personnel; and
- d. The information to be seized consists of communications and records regarding activities committed in furtherance of the crime of communicating threats, including records relating to the identities of those who created, used, or communicated with the account.

43. I am advised that, pursuant to 18 U.S.C. § 2703(a), a Court with jurisdiction over the offense that is under investigation has authority to issue a warrant to compel disclosure of stored content and records and other information pertaining to a customer or subscriber of an electronic communication service including a provider located physically in another judicial district. Accordingly, this Court has the authority to issue a warrant to Facebook for stored content and records and other information pertaining to its subscribers even though that business is located in California.

Conclusion

44. Based on the foregoing, there is probable cause to believe that within the contents of accounts **100011407980766** ("Hodeman Mujahid") and **100009118829119** ("Mahajir Zalmi"), that are stored at the premises of Facebook, Inc., a company located at 1601 S. California Avenue, in Palo Alto, California, there are communications, messages, and other

information, more particularly described in Attachment A, related to communicating threats, in violation of 18 U.S.C. § 875.

Wherefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure directed to Facebook, Inc. allowing agents to seize the information on the servers of that corporation, pursuant to the procedure outlined above.


I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

FURTHER THIS AFFIANT SAYETH NOT.



Mario A. Fratantonio
Special Agent, FBI

Subscribed to and sworn before me on this 26th day of May 2016.

_____/s/ 
Michael S. Nachmanoff
United States Magistrate Judge

MICHAEL S. NACHMANOFF
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

A. Facebook, Inc. personnel shall isolate the information associated with Account **100011407980766** with the user name "Hodeman Mujahid" and Account **100009118829119** with the user name Mahajir Zalmai, and provide in electronic form to the agent who serves the search warrant an exact duplicate of that information. With respect to each account, this information includes:

- (a) All contact and personal identifying information, including passwords, security questions and answers, and screen names;
- (b) All activity logs and all other documents showing the user's posts and other Facebook activities, and all photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (c) All Photoprints and Neoprints, including profile information and all photos uploaded by that user ID or by any user that have that user tagged in them, News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; all past and present friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (d) All records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests, as well as records of communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken; and all privacy settings and other account settings, and all records showing which Facebook users have been blocked by the account;
- (e) All "check ins" and other location information, and all IP logs, including all records of the IP addresses that logged into the account;
- (f) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked" and all information about the Facebook pages that the account is or was a "fan" of; and all records of Facebook searches performed by the account, and all information about the user's access and use of Facebook Marketplace;
- (g) All records of the length of service, the types of service utilized by the user, and the means and source of any payments associated with the service, and all cookie data and associate machines and accounts collected by Facebook for user's account to include, but not limited to, browser information if available and other pages and groups where the user (or the associated user) is the creator.

B. Law enforcement personnel will thereafter review all information and records received from Facebook, Inc. employees to determine the information to be seized by law enforcement personnel. The information to be seized consists of communications and records regarding activities committed in furtherance of the crime of making threatening communications in violation of 18 U.S.C. § 875.

ELECTRONIC EVIDENCE & SEARCH WARRANT TRANSMITTAL FORMCase No. 17 SW 178Date: December 20, 2020(S)AUSA: Kromberg 299-3721**I. TYPE OF LEGAL REQUEST:**

<input type="checkbox"/> ECPA Grand Jury Subpoena and Non-Disclosure Order (§§ 2703(c)(2), 2705(b))	<input type="checkbox"/> PRTT/Search Warrant Hybrid (§§ 3122(a)(1), 2703(c)(1)(A))
<input type="checkbox"/> ECPA Court Order (§ 2703(d))	<input type="checkbox"/> Regular Search Warrant (Rule 41(e)(2)(A))
<input type="checkbox"/> ECPA Content Search (§ 2703(a), (b)(1)(A))	<input type="checkbox"/> ESI Search Warrant (Rule 41(e)(2)(B))
<input type="checkbox"/> Pen Register/Trap & Trace (§ 3122(a)(1))	<input type="checkbox"/> Tracking Device Search Warrant (Rule 41(e)(2)(C))
<input checked="" type="checkbox"/> Other <u>Application for renewal of a NDO for a ESI Search Warrant</u>	

II. TYPE OF COMMUNICATIONS DEVICE/ACCOUNT:

<input type="checkbox"/> Cell Phone(s)	<input type="checkbox"/> Social Media/Messaging Account(s)
<input type="checkbox"/> Land Line(s)	<input type="checkbox"/> Computer(s)/Laptop(s)/Hard Drive(s)
<input checked="" type="checkbox"/> Email Account(s)	<input type="checkbox"/> Tracking Device(s)/Real-Time Cell Site Info
<input type="checkbox"/> IP Address(es)	<input type="checkbox"/> Other _____

III. INVESTIGATIVE OFFENSE:

<input type="checkbox"/> Drugs	<input type="checkbox"/> Sex Offenses
<input type="checkbox"/> Extortion/Racketeering	<input type="checkbox"/> Tax
<input type="checkbox"/> Fraud	<input checked="" type="checkbox"/> Terrorism
<input type="checkbox"/> Fugitive/Escape	<input type="checkbox"/> Theft
<input type="checkbox"/> Immigration	<input type="checkbox"/> Weapons
<input type="checkbox"/> Kidnapping	<input type="checkbox"/> Other _____

IV. DELAYED NOTICE:

<input type="checkbox"/> ECPA Non-Disclosure (§§ 2703(d), 2705(b))	<input type="checkbox"/> Search Warrant Delayed Notice (§ 3103a(b), Rule 41(f)(3))
<input type="checkbox"/> Initial – 1 year <input checked="" type="checkbox"/> Renewal	<input type="checkbox"/> Rule 41(e)(2)(A), (B), <u>or</u> (C) Warrants
<input type="checkbox"/> ECPA Non-Disclosure for Priority Terrorism Enterprise Investigations (§§ 2703(d), 2705(b))	<input type="checkbox"/> § 2703(a), (b)(1)(A), <u>or</u> (c)(1)(A) Searches
<input type="checkbox"/> Initial – 2 years <input type="checkbox"/> Renewal	_____ Days
	_____ Days Extension